

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 043034/0164

#7
B
02/17/04

Applicant: Kazue SAKO
Title: ANONYMOUS PARTICIPATION AUTHORITY MANAGEMENT SYSTEM
Serial No.: 09/765,390
Filed: January 22, 2001
Examiner: Gregory A. Morse
Art Unit: 2131

RECEIVED

FEB 13 2004

Technology Center 2100

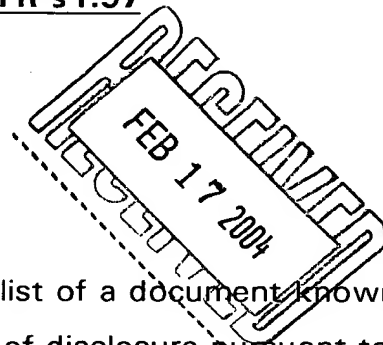
**INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §1.56 and 37 CFR §1.97**

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Submitted herewith on Form PTO-SB08 is a list of a document known to Applicant in order to comply with Applicant's duty of disclosure pursuant to 37 CFR 1.56. A copy of each listed document is being submitted to comply with the provisions of 37 CFR 1.97 and 1.98.

The submission of any document herewith, which is not a statutory bar, is not intended as an admission that such document constitutes prior art against the claims of the present application or that such document is considered material to patentability as defined in 37 CFR §1.56(b). Applicant does not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference any documents which is determined to be a prima facie prior art reference against the claims of the present application.



TIMING OF THE DISCLOSURE

The instant Information Disclosure Statement is believed to be filed in accordance with 37 C.F.R. 1.97(b), prior to the mailing date of a first Office Action on the merits (first scenario). If that is not the case, such as in a second scenario in which a first Office Action on the merits has been mailed before the filing of the instant Information Disclosure Statement, then either a certification or fee is required, and a certification is provided below. If neither of the first or second scenarios is the case, such as if a final Office Action or a notice of allowance has been mailed by the PTO (third scenario), then both a certification and fee are required, and in that case a certification is provided below and also the PTO is authorized to obtain the necessary fee to have the instant IDS considered, from Foley & Lardner Deposit Account #19-0741.

CERTIFICATION

The undersigned hereby certifies in accordance with 37 C.F.R. §1.97(e)(1) that each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three (3) months prior to the filing of this Statement.

RELEVANCE OF EACH DOCUMENT

A translation of a portion of a Japanese Office Action that issued December 26, 2003 with respect to a counterpart Japanese patent application is provided below.

"Although the function of providing an anonymous participant authorization management system is stated in Claim 1, it is not stated how the hardware resources will be specifically used in order to realize the function in question, and therefore, it cannot be confirmed that the hardware resources work in conjunction with the information processing based on software.

With this in view, we can find no creativity of a technical concept that uses a natural principle, and therefore the invention of Claim 1 does not qualify as an "invention" as defined in Article 2 of the Japan Patent Law.

Claim: 1

Cited Literature: 1

Remarks

Described in Cited Literature 1 is a voting system consisting of voters V_i ($i=1, \dots, I$), and election managers A_1, \dots, A_J , wherein the voter V_i uses random number r_j ; m_J, \dots, m_1 is calculated from the vote contents $v_i (=m_{J+1})$; the voter's own name $s_{v_i}(m_1)$ is added and sent to an election manager A_1 ; the election manager A_1 verifies the correctness of $s_{v_i}(m_1)$; and it is confirmed that vote approval has not yet been received. For $j=1, \dots, J-1$, A_j repeatedly conducts processing that calculates m_{j+1} from the m_j received and sends this in random order to A_{j+1} . A_J lists the v_i in random order together with the vote results of other voters. (Refer to pages 243 to 244 16.4 Mixnet use method.)

The invention related to Claim 1 will be compared with the invention described in Cited Literature 1.

The "voter V_i " and "election manager A_1 " in the invention described in Cited Literature 1 are equivalent to the "participant subsystem" and "receiving subsystem" in the invention related to Claim 1.

In the invention described in Cited Literature 1, the fact that m_{J+1}, \dots, m_1 is calculated using random number r_j is what anonymizes the voter even when multiple votes are cast, and this corresponds to "anonymous participation is possible wherein the participant subsystem is not detected even if participation spans multiple sessions using the aforementioned confidential information" in the invention related to Claim 1.

In the invention described in Cited Literature 1, the point of the fact that the voter attaches his own name $s_{v_i}(m_1)$ and sends this to the election manager A_1 is that the participant signs individual information using a secret key, and this anonymizes which voter signed which individual information because, for $j=1, \dots, J-1$, election manager A_j repeatedly conducts processing that calculates m_{j+1} from the m_j received and sends this in random

order to $A_j + 1$. This corresponds to "the participant subsystem having an anonymous name function to authorize individual information in conjunction with participation using a secret key in relation to the session of participation" in the invention related to Claim 1.

"The election manager A1 verifies the correctness of $sVi(m1)$ " and "it is confirmed that vote approval has not yet been received" in the invention described in Cited Literature 1 correspond respectively to "the receiving subsystem verifies that the information sent is anonymous and that a participant subsystem authorized to participate has attached an authorized anonymous signature," and "it is determined whether or not the same participant subsystem has signed information sent with two optional anonymous signatures" in the invention related to Claim 1.

There is a difference between the two inventions on the points that, in contrast to the fact that the invention related to Claim 1 provides "a manager subsystem," and that the participant subsystem "has secret information given by the manager subsystem, and has authorization to participate ... using this secret information," whether the invention described in Cited Literature 1 is made in these ways is unclear. All other points agree.

When studying the above points of difference, the fact that participant authority is given by the manager giving the participant secret information is nothing more than well-known, customary technology widely and generally used at the time of submitting this application.

Consequently, the invention related to Claim 1 could be easily applied by a person skilled in the art based on the invention described in Cited Literature 1.

List of Cited Literature

1. Ryuaki Okamoto, Hiroshi Yamamoto, "Modern Encrypting," Sangyo Zusho Co., Ltd., June 30, 1997, p. 243 to 244.

Record of Prior Art Literature Search Results

Fields searched - IPC 7th Edition - G09C 1/00."

Applicant's statements regarding the Japanese Office Action are based on a partial translation that Applicant's representative obtained. These statements should in no way be considered as an agreement by Applicant with, or an admission of, what is asserted in the Japanese Office Action.

Applicant respectfully requests that the listed document be considered by the Examiner and formally be made of record in the present application and that an initialed copy of Form PTO/SB/08 be returned in accordance with MPEP §609.

Respectfully submitted,

February 12, 2004
Date

Phillip J. Articola
Phillip J. Articola
Registration No. 38,819

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5143
Telephone: (202) 672-5300
Facsimile: (202) 672-5399